

Entanglement and output entropy of the diagonal map

Meik Hellmund

*Mathematisches Institut, Universität Leipzig, Johannisgasse 26, D-04103 Leipzig, Germany**

We review some properties of the convex roof extension, a construction used, e.g., in the definition of the entanglement of formation. Especially we consider the use of symmetries of channels and states for the construction of the convex roof. As an application we study the entanglement entropy of the diagonal map for permutation symmetric real $N = 3$ states $\omega(z)$ and solve the case $z < 0$ where z is the non-diagonal entry in the density matrix. We also report a surprising result about the behaviour of the output entropy of the diagonal map for arbitrary dimensions N ; showing a bifurcation at $N = 6$.

PACS numbers: 03.67.-a, 03.67.Mn

I. INTRODUCTION

Let $\Phi: \omega \mapsto \omega'$ be a quantum channel or, somewhat more general, a trace-preserving positive map of (mixed) states $\omega \in \Omega$ from one quantum system Ω to states $\omega' \in \Omega'$ from another system. We call

$$E_{\Phi}(\omega) = \min_{\omega = \sum p_j \pi_j} \sum_j p_j S(\Phi(\pi_j)) \quad (1)$$

entanglement entropy of the channel Φ or Φ -*entanglement* for short. Here the minimum is taken over all possible convex decompositions of the input state ω into pure states

$$\omega = \sum p_j \pi_j, \quad \pi_j \text{ pure, i.e., } \pi_j = |\psi_j\rangle\langle\psi_j| \quad (2)$$

and $S(\omega) = -\text{Tr } \omega \log \omega$ is the von Neumann entropy of the output states. We use the symbol \sum^c to denote a convex sum, i.e., it implies $p_j > 0$ and $\sum p_j = 1$.

The quantity (1) appears in different places in quantum information theory. For example,

1. The celebrated *entanglement of formation*[1] of a bipartite quantum system is the Φ -entanglement of the partial trace $\Phi = \text{Tr}_A$ with respect to one of the subsystems of the bipartite system.
2. The theorem of Holevo, Schumacher, and Westmoreland[2, 3] shows that the one-shot or product state classical capacity $\chi(\Phi)$ of a channel Φ can be obtained by maximising the difference between output entropy and entanglement entropy (the so-called Holevo quantity) over all input density operators:

$$\begin{aligned} \chi_{\Phi}^*(\omega) &= S(\Phi(\omega)) - E_{\Phi}(\omega) \\ \chi_{\Phi} &= \max_{\omega} \chi_{\Phi}^*(\omega) \end{aligned} \quad (3)$$

3. In [4] the optimization problem Eq. (1) was considered in connection with the quantum dynamical entropy of Connes-Narnhofer-Thirring[5]. In this framework one considers a subalgebra $\mathcal{B} \subset \mathcal{A}$ of the algebra \mathcal{A} of observables. The restriction of states to this subalgebra gives rise to a channel $\Phi_{\mathcal{B},\mathcal{A}}$, the dual of the inclusion map $\mathcal{B} \hookrightarrow \mathcal{A}$. The difference $S(\Phi(\omega)) - E_{\Phi}(\omega)$ is called *entropy of the subalgebra*; see also [6] for a thorough presentation.

Closed formulas for the entanglement entropy, i.e., analytic solutions to the global optimization problem Eq. (1) are very rare. They include certain classes of highly symmetric states [7–9] and the celebrated entanglement of formation of a pair of qubits[10].

Even earlier, Benatti, Narnhofer and Uhlmann [4, 11, 12] studied the entanglement entropy of the diagonal map of a 3-dimensional quantum system as an example for the entropy of a subalgebra. The diagonal map (also called

*Electronic address: Meik.Hellmund@math.uni-leipzig.de

pinching channel) Φ_D sets all non-diagonal elements of the input state ω to zero and corresponds to the choice of a maximal abelian subalgebra $\mathcal{B} \subset \mathcal{A}$. Using a mixture of analytical and numerical methods, they found explicit results for the entanglement entropy E_{Φ_D} (called E_D in what follows) of the diagonal map Φ_D applied to the one-dimensional family of permutation symmetric $N = 3$ real input states

$$\omega(z) = \frac{1}{3} \begin{pmatrix} 1 & z & z \\ z & 1 & z \\ z & z & 1 \end{pmatrix}. \quad (4)$$

In this paper we present some remarks about the role of symmetries in the optimization problem (1) based on the observations in [7, 8]. Using those insights we provide new results for the entanglement entropy $E_D(z)$ of states of the form (4) for the case of negative values of the parameter z .

We also present a result about the output entropy of the diagonal map in arbitrary dimensions.

II. CONVEX HULLS AND ROOF EXTENSIONS

The state space Ω of a quantum mechanical system with an N -dimensional Hilbert space \mathcal{H} is a compact convex space of $N^2 - 1$ real dimensions.

A (*proper*) *face* F of Ω is a non-empty subset $F \subsetneq \Omega$ which is closed under convex compositions and decompositions, i.e., whenever $\omega = \sum_i^c p_i \omega_i$ and $\omega \in F$, then $\omega_i \in F$. The (non-disjoint) union of all faces $\bigcup F_i = \partial\Omega$ constitutes the boundary of Ω . There is a one-to-one correspondence between the faces of Ω and linear subspaces of \mathcal{H} with an $K^2 - 1$ -dimensional face for every K -dimensional subspace. The face consists of all the states ω with support in the corresponding subspace. Zero-dimensional faces correspond to pure states and constitute the *extreme boundary* $\partial_e\Omega \subseteq \partial\Omega$.

Let $f(\omega)$ be a real-valued function on Ω . The convex hull f^\cup of f is the largest convex function not larger than f , i.e., for which $f^\cup(\omega) \leq f(\omega) \forall \omega \in \Omega$. The convex hull of a function is the solution of the global optimization problem

$$f^\cup(\omega) = \min_{\sum p_i \omega_i = \omega}^c \sum p_i f(\omega_i) \quad (5)$$

where the minimum is taken over all convex decompositions of ω . Carathéodory's theorem asserts that we can restrict the search for optimal decompositions to decompositions of length up to $l_{\max} = \dim \Omega + 1$.

Let us now consider the case where the function f is concave, such as the von Neumann entropy $S(\omega)$. Obviously we can then restrict the search for an optimal decomposition to the extremal boundary, $\omega_i \in \partial_e\Omega$. It follows that the convex hull f^\cup depends only on the values of f on $\partial_e\Omega$ and not on the behaviour of f inside Ω , as long as f is everywhere concave.

Therefore we can consider an extension problem which is closely related to the global optimization problem (5): Given a function $g(\pi)$ on $\partial_e\Omega$, i.e., on the set of pure states, we ask for a canonical extension g^\cup of g to all of Ω defined as

$$g^\cup(\omega) = \min_{\omega = \sum p_j \pi_j}^c \sum p_j g(\pi_j) \quad (6)$$

. This extension was called *convex roof extension* and intensively studied in, e.g., [13, 14]. It is, in a sense, the extension which is as linear as possible while being everywhere convex.

Definition II.1 (roof extension). A function $G(\omega)$ is called a *roof extension* of $g(\pi)$ if for every $\omega \in \Omega$ there is at least one extremal convex decomposition

$$\omega = \sum p_j \pi_j, \quad \pi_j \in \partial_e\Omega \quad (7)$$

$$\text{such that } G(\omega) = \sum p_j g(\pi_j). \quad (8)$$

If this is the case, we call the decomposition (7) *optimal* with respect to g or g -optimal.

Fig. 1 may illustrate the concept and explain the name. In a roof extension, the ground floor Ω is covered by straight roof beams and plane tiles. Those beams and tiles rest with their ends on the wall erected by $g(\pi)$. It is immediately clear from the definition of convexity that every convex extension is pointwise majorized by every roof extension. But is the largest convex extension a roof? The following theorem asserts that this is true at least when g is continuous and Ω compact:

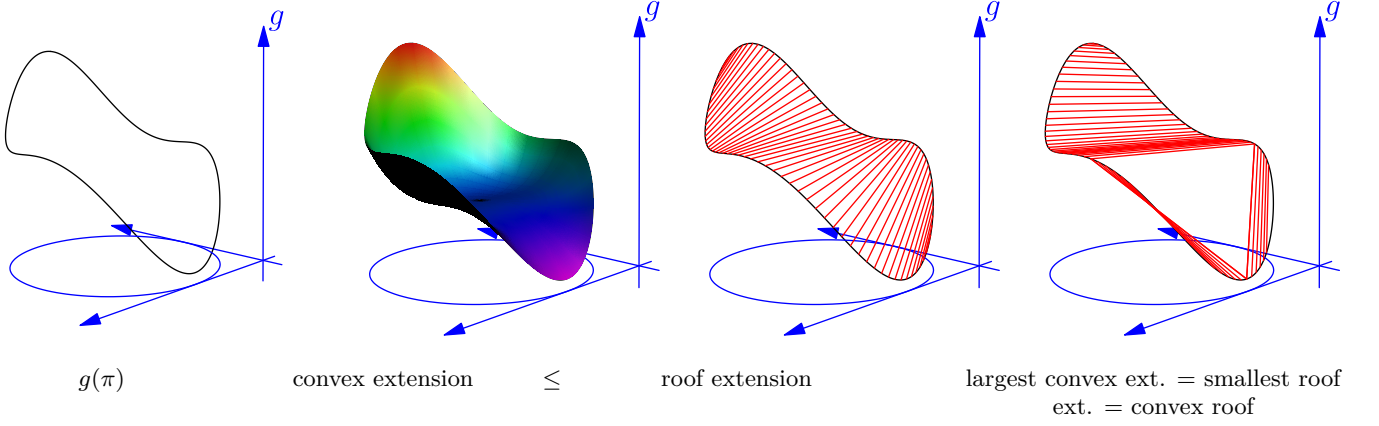


FIG. 1: An illustration of the convex roof extension where Ω is a disc and $\partial_e \Omega$ a circle.

Theorem II.1 ([4, 13]). *Let $g(\pi)$ be a continuous real-valued function on the set of pure states $\partial_e \Omega$. There exists exactly one function $g^\cup(\omega)$ on Ω which can be characterized uniquely by each one of the following four properties:*

1. g^\cup is the unique convex roof extension of g .
2. $g^\cup(\omega)$ is the solution of the optimization problem

$$g^\cup(\omega) = \inf_{\omega = \sum p_j \pi_j} \sum p_j g(\pi_j). \quad (9)$$

3. $g^\cup(\omega)$ is largest convex extension as well as the smallest roof extension of g .

Furthermore, given $\omega \in \Omega$, the function g^\cup is convex-linear on the convex hull of all pure states π appearing in optimal decompositions of ω .

Therefore, g^\cup provides a foliation of Ω into compact leaves such that a) each leaf is the convex hull of some pure states and b) g^\cup is convex-linear on each leaf.

Remark II.1. 1. The theorem justifies to write “min” instead of “inf” in Eqs. (1) and (9).

2. If g^\cup is not only linear but even constant on each leaf, it is called a flat roof.
3. Let $f(\omega)$ be a concave function on Ω , e.g., $f(\omega) = S(\Phi(\omega))$. Then we denote by f^\cup the convex roof extension of $f|_{\partial_e \Omega}$.

III. SYMMETRIES AND INVARIANT STATES

The following lemma gives a simple bound for f^\cup . Let $P : \Omega \rightarrow \Xi$ be an affine and surjective map $\omega \mapsto \xi$. The space Ξ , as the image of Ω under an affine map, is convex and compact, but it need not be a quantum state space. The map P provides a foliation of Ω into leaves $\Omega = \bigcup_{\xi \in \Xi} L_\xi$ via

$$L_\xi = \{\omega \mid \omega \in \Omega, P(\omega) = \xi\}. \quad (10)$$

Since P is affine, every leaf is generated by cutting Ω with some hyperplane and therefore, the leaves are convex, too. We define the function $\epsilon(\xi)$ on Ξ as the minimum of f on the corresponding leaf

$$\epsilon(\xi) = \min_{L_\xi} f(\omega) = \min\{f(\omega) \mid P\omega = \xi\}. \quad (11)$$

Lemma III.1. *The convex hull of the ϵ function, $\epsilon^\cup(\xi)$, provides a lower bound for the convex roof $f^\cup(\omega)$, i.e.,*

$$f^\cup(\omega) \geq \epsilon^\cup(P\omega) \quad (12)$$

Proof. Let $\omega = \sum \lambda_i \omega_i$ be optimal for f^\cup , so $f^\cup(\omega) = \sum \lambda_i f(\omega_i)$. Let $\xi_i = P\omega_i$. Then, due to linearity of P we have $\xi = \sum \lambda_i \xi_i$ and due to the definition of $\epsilon(\xi)$ we have $f(\omega_i) \geq \epsilon(\xi_i)$. So,

$$f^\cup(\omega) = \sum \lambda_i f(\omega_i) \geq \sum \lambda_i \epsilon(\xi_i) \quad (13)$$

and from eq. (5), we have

$$\sum \lambda_i \epsilon(\xi_i) \geq \epsilon^\mathbb{U}(\xi). \quad (14)$$

□

There are some cases where we can find states ω for which the inequality of the lemma can be sharpened to an equality.

Theorem III.2. *Let $P = P^2$ be a linear and idempotent map of the state space onto itself with a fixed point set $P\Omega = \Xi \subset \Omega$ of P -invariant states. Let $f(\omega)$ be P -invariant, i.e.,*

$$f(P\omega) = f(\omega) \quad \forall \omega \in \Omega \quad (15)$$

Then for all P -invariant states $\omega_P \in P\Omega$ holds

$$f^\cup(\omega_P) = \epsilon^\mathbb{U}(\omega_P) = \epsilon^\cup(\omega_P) \quad (16)$$

and these states have an optimal decomposition completely in $P\Omega$, i.e., into P -invariant states only. Furthermore, for every state ω it holds that

$$f^\cup(\omega) \geq f^\cup(P\omega) \quad (17)$$

Proof. Since f is P -invariant, it is constant on every affine subspace $P^{-1}\omega$. Therefore, we have $\epsilon(\omega) = f(\omega)$ on $P\Omega$ and ϵ is concave. So, $\epsilon^\mathbb{U}(\omega) = \epsilon^\cup(\omega)$. Let $\omega = {}^c \sum \lambda_j \omega_j$ be optimal for ϵ^\cup . Then,

$$\epsilon^\cup(\omega) = {}^c \sum \lambda_j \epsilon(\omega_j) = {}^c \sum \lambda_j f(\omega_j) \geq f^\cup(\omega). \quad (18)$$

Together with Lemma III.1 this proves (16) and provides an f^\cup -optimal decomposition lying in $P\Omega$. □

Example III.1. Let P be the projection to real states $P(\omega) = 1/2(\omega + \omega^\top)$ and f the output entropy of the diagonal map $S_{\text{out}}^D(\omega) = S(\Phi_D(\omega))$. Then real states have optimal decompositions into real states only. Furthermore, Lemma III.1 asserts that all non-real states have an entanglement entropy at least as large as their real projections

$$E_D(\omega) = f^\cup(\omega) \geq \epsilon^\cup(P\omega) = E_D(P\omega) \quad \forall \omega \in \Omega \quad (19)$$

A slightly different version was used in [7] and worked out in [8]:

Theorem III.3 ([7, 8]). *Let G be a symmetry group of f such that $f(\omega^g) = f(\omega)$ for all $\omega \in \Omega$ and $g \in G$. Let P_G be the twirl map or group average corresponding to G , i.e., the idempotent projection to the subspace $P_G\Omega$ of G -invariant states*

$$\omega_P = P_G\omega = \frac{1}{|G|} \sum_{g \in G} \omega^g \quad (20)$$

Then for all G -invariant states $\omega_P \in P_G\Omega$ holds

$$f^\cup(\omega_P) = \epsilon^\mathbb{U}(\omega_P). \quad (21)$$

Furthermore, for every state $\omega \in \Omega$ it holds that

$$f^\cup(\omega) \geq f^\cup(P\omega) \quad (22)$$

States ω_P for which $\epsilon^\mathbb{U}(\omega_P) = \epsilon(\omega_P)$ have an optimal decomposition consisting of one complete orbit of G ; otherwise the optimal decomposition consists of several complete orbits.

Proof. We assume that $\omega_P = \sum \lambda_i \omega_i$ is optimal for $\epsilon^\cup(\omega_P)$. Let $\tilde{\omega}_i$ be states which achieve the minimum in eq. (11) for the ω_i : $\epsilon(\omega_i) = f(\tilde{\omega}_i)$ and $\tilde{\omega}_i$ belongs to the leaf L_i . So, $P\tilde{\omega}_i = \omega_i$ and therefore

$$\omega_P = \sum_{i,g} \frac{\lambda_i}{|G|} \tilde{\omega}_i^g \quad (23)$$

is a candidate decomposition for f . So,

$$f^\cup(\omega_P) \leq \sum_{i,g} \frac{\lambda_i}{|G|} f(\tilde{\omega}_i^g) \quad (24)$$

With $f(\omega^g) = f(\omega)$ and $\sum_g \frac{1}{|G|} = 1$, the right hand side evaluates to

$$f^\cup(\omega_P) \leq \sum_i \lambda_i f(\tilde{\omega}_i) = \sum_i \lambda_i \epsilon(\omega_i) = \epsilon^\cup(\omega) \quad (25)$$

This, together with lemma III.1, proves the theorem and shows that decomposition (23) is optimal for f^\cup . \square

Please note that the G -invariance of f does not imply P_G -invariance of f . This is the main difference between Theorem III.2 and Theorem III.3 for applications.

Only in the case where $f(\omega)$ is P_G -invariant $f(P\omega) = f(\omega)$ (which implies G -invariance $f(\omega^g) = f(\omega)$) we know that every G -invariant state has an optimal decomposition consisting solely of G -invariant states.

IV. OUTPUT ENTROPY OF THE DIAGONAL MAP

The diagonal map Φ_D maps Ω_N , the state space of an N -dimensional Hilbert space, to the simplex $\Omega'_N = \{x_1, x_2, \dots, x_N\}$, $0 \leq x_i \leq 1$, $\sum x_i = 1$. It corresponds to a complete von Neumann measurement. Its Kraus form is

$$\Phi(\omega) = \sum_{i=1}^N P_i \omega P_i \quad (26)$$

with $P_i = |i\rangle\langle i|$. The output entropy of this channel is

$$S_{\text{out}}^D(\omega) = S(\Phi_D(\omega)) \quad (27)$$

$$= \sum_{i=1}^N \eta(x_i) \quad (28)$$

with the usual abbreviation $\eta(x) = -x \log(x)$ for $x > 0$ and $\eta(0) = 0$. This function is not only concave but a concave roof, as was shown in [14].

The minimal output entropy is zero and the maximal one is $\log N$.

Things become more refined by restricting the channel onto a face of Ω_N . As an example we take the $(N-1)$ -dimensional subspace \mathcal{H}_0 which is orthogonal to the vector $|\phi\rangle = N^{-1/2} \sum |j\rangle$. It consists of vectors $\sum a_j |j\rangle$ such that $\sum a_j = 0$. \mathcal{H}_0 supports pure states satisfying $\Phi_D(\pi) = N^{-1} \mathbb{1}$ and so the maximal output entropy is $\log N$ again.

For the minimal output entropy we have a more complex result:

Theorem IV.1. *Let Ω_0 be the face of Ω_N consisting of states whose support is orthogonal to $\sum_{i=1}^N |i\rangle$. Let S_{\min}^D be the minimal output entropy of the diagonal map Φ_D . Then we have:*

- We have $S_{\min}^D(\Omega_0) = \log 2$ for $N = 2, 3, \dots, 6$. This is achieved by the $N(N-1)/2$ pure input states π_{jk} , $j < k$, and only by these states. Here, $\pi_{jk} = |\phi_{jk}\rangle\langle\phi_{jk}|$ with $|\phi_{nm}\rangle = 2^{-1/2}(|n\rangle - |m\rangle)$.
- For $N > 6$ we have

$$S_{\min}^D(\Omega_0) = \log N - \left(1 - \frac{2}{N}\right) \log(N-1) \quad (29)$$

and $\lim_{N \rightarrow \infty} S_{\min}^D = 0$. The minimum is achieved by the N states $\pi_j = |\phi_j\rangle\langle\phi_j|$ where

$$\phi_1 = ((N-1)a, -a, -a, \dots, -a) \quad \text{with} \quad a = (N(N-1))^{-1/2} \quad (30)$$

and the other ϕ_i are obtained by permuting the components.

The proof of this theorem is found in the appendix.

V. ENTANGLEMENT ENTROPY OF THE $N = 3$ DIAGONAL MAP FOR SOME SUBSETS OF STATES

A. Geometry of the $N = 3$ state space

The space Ω_3 of positive hermitean 3×3 matrices with unit trace has 8 real dimensions. Its boundary consists of zero-dimensional faces (pure states) and three-dimensional faces (Bloch balls), the latter corresponding to two-dimensional subspaces of the Hilbert space $\mathcal{H} = \mathbb{C}^3$.

We will use the notion $\psi = (a, b, c)$ to denote a one-dimensional subspace $[\mathbb{C}\psi]$ of \mathbb{C}^3 as well as the corresponding point $\pi_\psi = |\psi\rangle\langle\psi|$ of Ω_3 . Here, (a, b, c) is a generally unnormalized element of this one-dimensional subspace. The set of states orthogonal to a given pure state ψ form a Bloch ball which we denote by $B^\perp(\psi)$:

$$B^\perp(\psi) := \{\omega \mid \langle\psi|\omega|\psi\rangle = 0\} \quad (31)$$

and all non-trivial faces of Ω_3 are obtained in this way: There is a Bloch ball opposite to each pure state and this gives a bijection between the 0- and 3-dimensional faces of Ω .

More generally, we can consider for every pure state ψ the foliation of Ω_3 by parallel hyperplanes $L_\psi(F)$ defined as

$$L_\psi(F) := \{\omega \mid \langle\psi|\omega|\psi\rangle = F\} \quad (32)$$

where F is the fidelity parameter. The leaves are 7-dimensional in the generic case, but the highest leaf $L_\psi(1) = \pi_\psi$ consist of one pure state only and the lowest leaf $L_\psi(0) = B^\perp(\psi)$ is the Bloch ball opposite to ψ . Furthermore, every basis $\{\psi_1, \psi_2, \psi_3\}$ of three orthogonal pure states spans an equilateral triangle in Ω_3 . Every edge $\overline{\psi_i\psi_j}$ of this triangle is the diameter of the Bloch ball $B^\perp(\psi_k)$ orthogonal to the opposite vertex, see Fig. 2. All these triangles have the

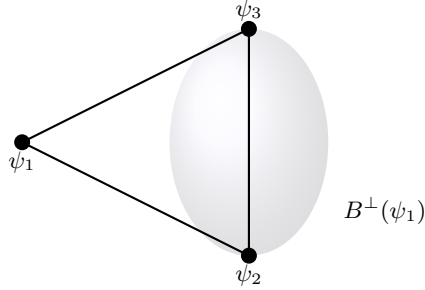


FIG. 2: Bloch ball face and opposite face. Note that the plane of the triangle and the ball have only a one-dimensional intersection, the diameter $\overline{\psi_2\psi_3}$

barycenter $1/3$ of Ω in common.

B. States of lowest entanglement entropy

The triangle spanned by the computational basis $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ is the lowest leaf of the roof of $E_D = S_D^\cup$, the leaf where $E_D = 0$. Especially, $E(1/3) = 0$. This triangle is the fixed point set of the diagonal channel Φ_D .

C. Some rank-2 states

We can calculate E_D for every Bloch ball which includes one of the three states of the computational basis. Take, for example, $B(\psi_0, \psi_{ab})$, the ball spanned by $\psi_0 = (1, 0, 0)$ and some orthogonal state $\psi_{ab} = (0, a, b)$. This ball is the image of the unitary embedding $V: \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ a \\ b \end{pmatrix}$ of a standard Bloch ball. This embedding can be used to reduce the calculation of the convex roof to the $N = 2$ case, see chapter 6.2 in [14]. Using the known results for the $N = 2$ diagonal map (see, e.g., [12]) we find for states from this Bloch ball, i.e., states of the form

$$\omega = \begin{pmatrix} 1-z & xa & xb \\ x^*a^* & za^*a & za^*b \\ x^*b^* & zab^* & zb^*b \end{pmatrix} \quad (33)$$

with real z and complex x, a, b the entanglement entropy

$$E_D = \eta\left(\frac{1+\lambda}{2}\right) + \eta\left(\frac{1-\lambda}{2}\right) + z\eta(a^*a) + z\eta(b^*b) \quad \text{where} \quad \lambda = \sqrt{1-4x^*x}. \quad (34)$$

D. Real permutation invariant states

The permutation group $G = S_3$ acts on Ω_3 by permuting the computational basis $\left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\}$. The corresponding twirl acts on normalized pure states $\psi = (a, b, c)$ as

$$P_G(\pi_\psi) = \frac{1}{3} \begin{pmatrix} 1 & z & z \\ z & 1 & z \\ z & z & 1 \end{pmatrix} \quad \text{where} \quad 2z = ab^* + a^*b + ac^* + a^*c + bc^* + b^*c. \quad (35)$$

Let us denote the S_3 -invariant state on the right hand side as $\omega(z)$. In what follows, we restrict our considerations to real states $\omega = \omega^\top$. Then the real parameter z can take values in the range

$$-\frac{1}{2} \leq z \leq 1. \quad (36)$$

Another often used parametrization for these states uses the fidelity with respect to the state $\omega(1) = \pi(1, 1, 1)$. We have

$$F = \langle \psi_{(1,1,1)} | \omega | \psi_{(1,1,1)} \rangle = \frac{1}{3}(2z + 1). \quad (37)$$

The state $\omega(z)$ is of rank three except at the boundaries of the z range:

- For $z = 1$ we have a pure state

$$\omega(1) = \pi(1, 1, 1) \quad (38)$$

where we use $\pi(a, b, c)$ as shorthand for the pure state $\pi_\psi = |\psi\rangle\langle\psi|$ with $\psi \sim (a, b, c)$. So its entanglement entropy equals its output entropy and we have

$$E_D(1) = \log(3). \quad (39)$$

- For $z = -1/2$ we have a rank-2 state

$$\omega(-1/2) = \frac{1}{2} [\pi(-1, 0, 1) + \pi(-1, 2, -1)]. \quad (40)$$

This state belongs to the face of Ω considered in Section IV, so its entanglement entropy can't be smaller than $\log(2)$. It is easy to see that this value can indeed be achieved by the optimal decomposition

$$\omega(-1/2) = \frac{1}{3} [\pi(1, 0, -1) + \pi(0, -1, 1) + \pi(-1, 1, 0)], \quad (41)$$

and therefore

$$E_D(-1/2) = \log(2) \quad (42)$$

- Let's also mention that for $z = 0$ we have the maximally mixed state which belongs to the lowest leaf of Section V B. So an optimal decomposition is

$$\omega(0) = \frac{1}{3} [\pi(1, 0, 0) + \pi(0, 1, 0) + \pi(0, 0, 1)], \quad (43)$$

$$E_D(0) = 0. \quad (44)$$

Applying Theorem III.2 using the projection $P\omega = \frac{1}{2}(\omega + \omega^\top)$ we see that the states $\omega(z)$ have optimal decompositions including only real states. Furthermore, for an arbitrary state we have

$$E_D(\omega) \geq E_D\left(\frac{\omega + \omega^\top}{2}\right). \quad (45)$$

Applying now Theorem III.3 with the projection P_G to the space of real states we learn that

$$E_D(z) = \epsilon^\Psi(z) \quad \text{where} \quad \epsilon(z) = \min_{P_G(\pi(a,b,c))=\omega(z)} S_D(\pi(a,b,c)), \quad \text{with } z, a, b, c \text{ real} \quad (46)$$

The minimization in Eq. (46) is one-dimensional since the three real parameters are constrained by $a^2 + b^2 + c^2 = 1$, $ab + bc + ac = z$. A useful parametrization of this constraint is [4]

$$3(a, b, c) = (\alpha + 2\beta \cos \theta, \alpha - 2\beta \cos(\theta - \pi/3), \alpha - 2\beta \cos(\theta + \pi/3)) \quad \text{where} \quad \alpha = \sqrt{2z+1}, \beta = \sqrt{1-z} \quad (47)$$

Numerical search for the minimum in Eq. (46) shows that the minimum is reached at $\theta = 0$ for all $z > -0.4150234$. For smaller values of z , θ_{\min} increase up to $\theta_{\min} = \pi/6$ at $z = -1/2$. A thorough analysis of the function $\epsilon(z)$ obtained by this minimization shows that it is not everywhere convex. In the region $z \geq 0$ we re-obtained the result of [12]: the convex hull ϵ^Ψ is obtained by replacing $\epsilon(z)$ in the region $5/6 < z \leq 1$ with a linear piece.

In the negative- z region our results differ from [12], who claimed that $\epsilon(z)$ is convex there. We find that the convex hull is obtained by replacing $\epsilon(z)$ in the region between $z = -1/2$ and $z = z^* = -0.4079496711$ with a linear piece, see Fig. 3.

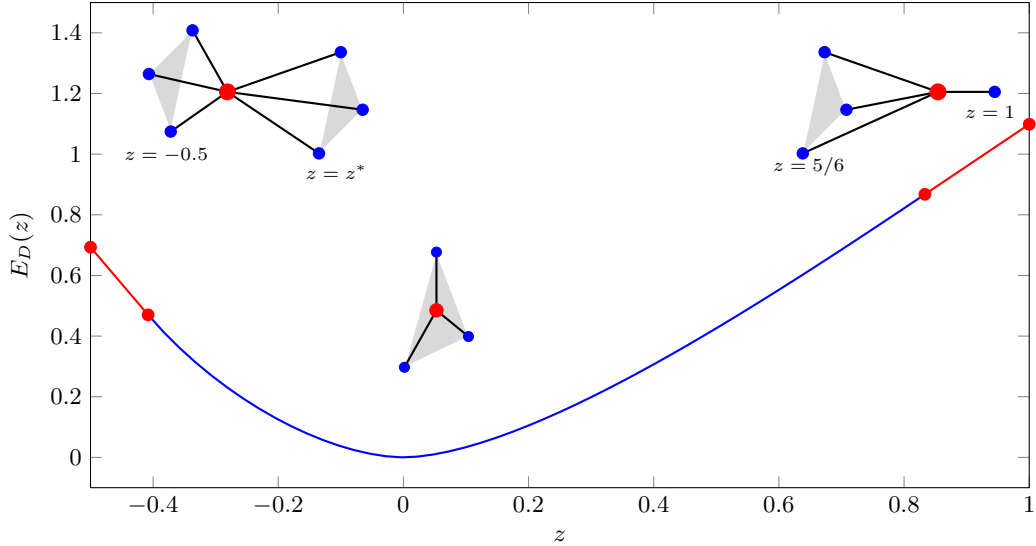


FIG. 3: Entanglement entropy and optimal decompositions. Regions where the convex hull construction leads to a linear behaviour are drawn in red. The drawings indicate the shape of optimal decompositions of the red state into pure (blue) states in the three regions $z < z^*$, $z^* \leq z < 5/6$, $5/6 < z$, resp. Here, gray surfaces indicate hyperplanes of states which project under P_G to the same value of z . The corners of the triangles form a complete orbit under the permutation group $G = S_3$.

Interestingly, everywhere in the region $z^* \leq z \leq 5/6$ where $\epsilon(z) = \epsilon^\Psi(z)$ the minimum is obtained for states with $\theta = 0$. So the optimal decompositions in this region have the form

$$\omega = \frac{1}{3} [\pi(a, b, b) + \pi(b, b, a) + \pi(b, a, b)], \quad (48)$$

corresponding to a short orbit of S_3 of length 3 only. In the region $-1/2 < z < z^*$ the optimal decomposition has length 6 and is a mixture of two such short orbits resulting in a large region in state space where the entanglement entropy is an affine function.

With

$$S(z) = 2\eta\left(\frac{(\alpha - \beta)^2}{9}\right) + \eta\left(\frac{(\alpha + 2\beta)^2}{9}\right) \quad \text{where} \quad \alpha = \sqrt{2z+1}, \beta = \sqrt{1-z} \quad (49)$$

and $z^* = -0.4079496711$, $\mathcal{S}(5/6) = \log(3) - 1/3 \log(2)$ the final result for the entanglement entropy is therefore

$$E_D(z) = \begin{cases} p \log(2) + (1-p)\mathcal{S}(z^*) & \text{for } -1/2 \leq z < z^* \text{ with } p = \frac{z^* - z}{z^* + 1/2} \\ \mathcal{S}(z) & \text{for } z^* \leq z \leq 5/6 \\ p[\log(3) - 1/3 \log(2)] + (1-p) \log(3) & \text{for } 5/6 < z \leq 1 \text{ with } p = \frac{1-z}{1-5/6} \end{cases} \quad (50)$$

Acknowledgments

I would like to thank Armin Uhlmann for encouragement and many useful explanations and discussions.

Appendix A: Proof of theorem IV.1

1. We have $S_{\text{out}}^D(\omega) = S_{\text{out}}^D(\omega^\top) = S_{\text{out}}^D(\frac{1}{2}(\omega + \omega^\top))$. Therefore we can restrict our search for the minimum to the subspace $\Omega_{\mathbb{R}} = \{\omega \mid \omega = \omega^\top\}$ of real states.
2. The minimal output entropy is attained by pure states since S_{out}^D is concave and $\Omega_{\mathbb{R}}$ is convex.
3. The case $N = 2$ is trivial. There is only one pure real state $\phi_{12} = \phi_1 = 2^{-1/2}(1, -1)$ in \mathcal{H}_0 with $S_{\text{out}}^D = \log 2$. So we now assume $N \geq 3$.
4. The pure real states in \mathcal{H}_0 have the form $\pi = |\psi\rangle\langle\psi|$ with

$$|\psi\rangle = \sum a_j |j\rangle, \quad \sum a_j = 0, \quad \sum a_j^2 = 1 \quad \text{which implies} \quad a_i \in (-1, 1). \quad (A1)$$

So we use Lagrange's multiplier method to find the minimum of

$$S_{\text{out}}^D(\pi) = - \sum a_j^2 \log a_j^2 \quad (A2)$$

for all a_i satisfying eq. (A1). The equations to solve read

$$a_i \log a_i^2 + a_i = \lambda + a_i \mu' \quad (A3)$$

$$\text{or:} \quad a_i \log a_i^2 = \lambda + a_i \mu \quad (A4)$$

where λ, μ' denote Lagrange multipliers for the constraints Eq. (A1) and $\mu = \mu' - 1$. Multiplying eq. (A4) by a_j and summing over j yields

$$S_{\text{out}}^D = -\mu \quad \text{and therefore,} \quad \mu < 0. \quad (A5)$$

Not all solutions of eq. (A4) have minimal output entropy but all states of minimal entropy must be solutions of eq. (A4). So can find the minimum by classifying all solutions and comparing their entropy. Let us consider different cases:

- (a) $\lambda = 0$, so the solutions of eq. (A4) are $a_i \in \{0, \pm \exp(\mu/2)\}$. Let m instances of the a_i be nonzero. Then their modulus must be $m^{-1/2}$ for $\sum a_j^2 = 1$ and $S_{\text{out}}^D = -\mu = \log m$. Since m must be even for $\sum a_j = 0$, the minimum value for S_D is achieved for $m = 2$. So one candidate for the minimum of S_{out}^D is

$$S_{\text{out}}^D = \log 2, \quad |\phi_{jk}\rangle = 2^{-1/2}(|j\rangle - |k\rangle) \quad (A6)$$

- (b) $\lambda \neq 0$. Then all the a_i have to be non-zero. The transcendental equation $\lambda + x\mu = x \log x^2$ can be rewritten as

$$\frac{\lambda}{2} e^{-\frac{\mu}{2}} = \frac{\lambda}{2|x|} e^{\frac{\lambda}{2x}} = \pm w e^w \quad \text{with} \quad w = \lambda/2x \quad (A7)$$

The inverse of the function $f(w) = w e^w$ is the Lambert W function $W(z)$ [15], defined via

$$z = W(x) e^{W(x)}. \quad (A8)$$

As an inverse of a non-injective function it has multiple branches, two of which are real and denoted as W_{-1} and W_0 . It follows that $\lambda + \mu x = x \log x^2$ has no more than three real solutions which can be expressed as

$$x_1 = \frac{\lambda}{2W_0(z)} \quad \text{where} \quad z = \frac{|\lambda|}{2} e^{-\mu/2} \quad (\text{A9})$$

$$x_2 = \frac{\lambda}{2W_0(-z)} \quad (\text{A10})$$

$$x_3 = \frac{\lambda}{2W_{-1}(-z)} \quad (\text{A11})$$

Since $\lambda \neq 0$ we have $z > 0$. Then a solution x_1 does always exist and the solutions x_2 and x_3 exist only if $z \leq 1/e$. They are equal for $z = 1/e$.

i. Let us assume that only two of the values, say x_1 and x_2 are used in the state. So we have

$$nx_1 + mx_2 = 0, \quad nx_1^2 + mx_2^2 = 1, \quad n + m = N, \quad n, m \geq 1 \quad (\text{A12})$$

resulting in $x_1^2 = \frac{m}{nN}$, $x_2^2 = \frac{n}{mN}$ and so

$$S(N, n) = \log N - \left(1 - \frac{2n}{N}\right) \log \left(\frac{N}{n} - 1\right) \quad (\text{A13})$$

Now this expression is concave in n :

$$\frac{\partial^2 S(N, m)}{\partial n^2} = -\frac{N^2}{n^2(N-n)^2} < 0 \quad \text{for} \quad 0 < n < N \quad (\text{A14})$$

and therefore takes for fixed N its minimum at the edges of the allowed n -range, $n = 1$ or, equivalently, $n = N - 1$.

So the second possibility for a minimum of S_{out}^D is

$$S_{\text{out}}^D = \log N - \left(1 - \frac{2}{N}\right) \log(N-1), \quad \{a_j\} = (a, a, \dots, a, (1-N)a) \quad (\text{A15})$$

ii. The last possibility is that all three roots x_1, x_2, x_3 occur among the a_i . Consider the function

$$F(\lambda, \mu) = x_1^2 + x_2^2 + x_3^2 \quad (\text{A16})$$

where the x_i are the three solutions of $\lambda + \mu x = x \log x^2$. Using Eqs. (A8,A9,A10,A11) we find

$$F(\lambda, \mu) = e^\mu \left(e^{2W_0(z)} + e^{2W_0(-z)} + e^{2W_{-1}(-z)} \right) \quad (\text{A17})$$

$$= e^\mu G(\lambda, \mu) \quad (\text{A18})$$

$$\text{where} \quad G(\lambda, \mu) = e^{2W_0(z)} + e^{2W_0(-z)} + e^{2W_{-1}(-z)} \quad (\text{A19})$$

Now we have $G(0) = 2$ and $G'(z) > 0$ for $z \in (0, 1/e]$ (see Fig. 4), therefore $G(z) > 2$ for $z \in (0, 1/e]$.

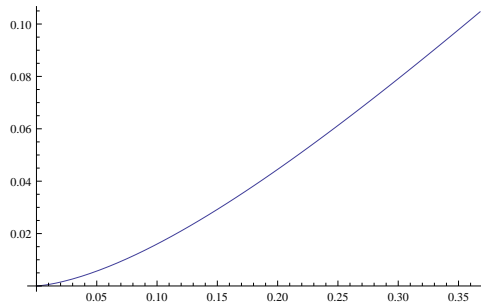


FIG. 4: Plot of $G'(z)$ over z

Since we need $F \leq 1$ for a normalized state vector, this implies $e^\mu < \frac{1}{2}$, $\mu < -\log 2$, $S_{\text{out}}^D = -\mu > \log 2$ and therefore any such solution has larger output entropy than the state given by Eq. (A6).

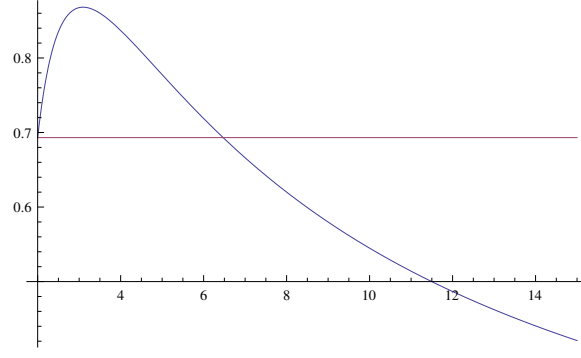


FIG. 5: The output entropies $\log 2$ and Eq. (A15) plotted over N

5. The only thing left to do is to compare the two candidates for a minimum, Eqs. (A15) and (A6). It is easy to see, that candidate (A6) wins for $N \leq 6$ and candidate (A15) wins for all $N > 6$, see Fig. 5. \square

-
- [1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Physical Review A* **54**, 3824 (1996), quant-ph/9604024.
 - [2] B. Schumacher and M. D. Westmoreland, *Phys. Rev. A* **56**, 131 (1997).
 - [3] A. S. Holevo, *IEEE Transactions on Information Theory* **44**, 269 (1998), quant-ph/9611023.
 - [4] F. Benatti, H. Narnhofer, and A. Uhlmann, *Rep. Math. Phys.* **38**, 123 (1996).
 - [5] A. Connes, H. Narnhofer, and W. Thirring, *Commun. in Math. Phys.* **112**, 691 (1987).
 - [6] F. Benatti, *Dynamics, Information and Complexity in Quantum Systems* (Springer, 2009).
 - [7] B. M. Terhal and K. G. H. Vollbrecht, *Phys. Rev. Lett.* **85**, 2625 (2000).
 - [8] K. G. H. Vollbrecht and R. F. Werner, *Phys. Rev. A* **64**, 062307 (2001), quant-ph/0010095.
 - [9] K. K. Manne and C. M. Caves, *Quantum Information & Computation* **8**, 295 (2008).
 - [10] W. K. Wootters, *Phys. Rev. Lett.* **80**, 2245 (1998), quant-ph/9709029.
 - [11] F. Benatti, H. Narnhofer, and A. Uhlmann, *Lett. Math. Phys.* **47** (1999).
 - [12] F. Benatti, H. Narnhofer, and A. Uhlmann, *J. Math. Phys.* **44**, 2402 (2003).
 - [13] A. Uhlmann, *Open Sys. Information Dyn.* **5**, 209 (1998), quant-ph/9701014.
 - [14] A. Uhlmann, *Entropy* **12**, 1799 (2010).
 - [15] R. Corless, G. Gonnet, D. Hare, D. Jeffrey, and D. Knuth, *Adv. in Computational Math.* **5**, 329 (1996).